

**Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision**

May 20, 2004

The Honorable Edward J. Markey
Ranking Minority Member
Subcommittee on Telecommunications
and the Internet
Committee on Energy and Commerce
House of Representatives
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding the actions that our agencies have undertaken to protect the privacy of individuals residing in the United States when their personal information is sent offshore by U.S. companies. You asked a series of questions about these outsourcing practices by financial institutions and the supervisory measures that our agencies apply to enforce U.S. privacy laws and regulations.

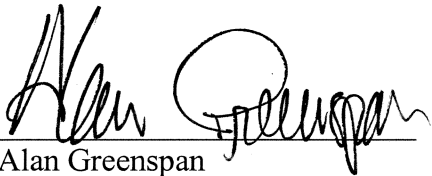
In responding to your general question, we note that many U.S. financial institutions often use service providers to perform various functions, such as data processing. The use of service providers, be they domestic or foreign-based, is a common business practice. Nevertheless, these outsourcing arrangements do raise certain risks to financial institutions. Our agencies expect U.S. financial institutions to effectively manage the risks associated with their outsourcing arrangements and comply with all applicable legal and regulatory requirements, regardless of whether these arrangements are with domestic or foreign firms. Specifically, the Federal Financial Institutions Examination Council (FFIEC) member agencies have stated their expectations that the boards of directors and senior management of financial institutions oversee and manage their outsourcing arrangements and institute outsourcing processes that comply with guidance issued by our agencies.¹

As explained more fully in the enclosed attachment prepared by our staff, our approach to supervising the cross-border outsourcing activities of financial institutions combines examinations with ongoing supervisory activities. Our principal supervisory strategy in this area is to focus on the ability and obligation of the financial institution to maintain controls over the privacy and security practices of its foreign-based service providers that possess or have access to its customer information.

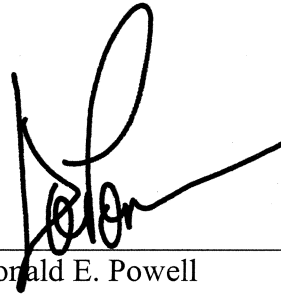
¹ The FFIEC member agencies are the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

You also asked whether we believe that a prohibition or severe limitation should be imposed on the ability of U.S. firms to transfer nonpublic personal information about American consumers to foreign-based service providers. At this time, we believe that the current supervisory framework for financial institutions is adequate to protect the privacy and security interests of their U.S. customers while also permitting institutions appropriate flexibility in using the services of foreign-based providers. Under this framework, our agencies can take effective supervisory actions with respect to any financial institution whose arrangement with a foreign-based service provider fails to comply with the requirements under U.S. law that relate to the privacy and security of its customer information.

Sincerely,



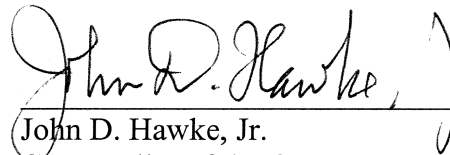
Alan Greenspan
Chairman
Board of Governors of the
Federal Reserve System



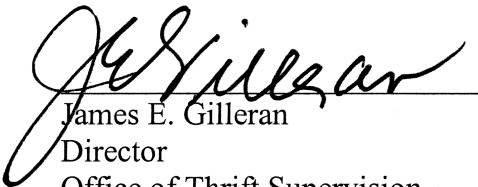
Donald E. Powell
Chairman
Federal Deposit Insurance Corporation



JoAnn Johnson
Chairman
National Credit Union Administration



John D. Hawke, Jr.
Comptroller of the Currency



James E. Gilleran
Director
Office of Thrift Supervision

Enclosure

**Response to an Inquiry by
The Honorable Edward J. Markey**

**The following information was prepared by staff of the member agencies of the
Federal Financial Institutions Examination Council**

The FFIEC agencies (Agencies) note that U.S. financial institutions often use domestic service providers to perform various functions, such as data processing. Increasingly, these institutions are also entering into servicing arrangements with foreign-based firms or domestic firms that subcontract portions of their operations to foreign-based entities.

The Agencies expect U.S. financial institutions to effectively manage the risks of their outsourcing arrangements, regardless of whether these are with domestic or foreign firms. Specifically, the Agencies have stated their expectations that the boards of directors and senior management of financial institutions oversee and manage their outsourcing arrangements and institute an outsourcing process that complies with guidance issued by the Agencies. *See, e.g.,* the FFIEC Policy on Risk Management of Outsourced Technology Services (2000).²

The use of foreign-based service providers, like domestic providers, is a common business practice. However, this outsourcing practice does raise certain risks, commonly classified as country,³ compliance, contractual, and reputation risks. Accordingly, the Agencies have advised (and will continue to advise) management of institutions using foreign-based service providers to: 1) conduct appropriate risk assessments, 2) maintain adequate due diligence procedures, 3) closely evaluate all contracts, and 4) establish ongoing monitoring and oversight procedures.⁴

Each of the agencies has issued guidance addressing the risks and appropriate practices with respect to outsourcing relationships. This general guidance applies to both domestic and foreign outsourcing arrangements, although some agencies have also issued guidance that specifically addresses foreign outsourcing. In accordance with this guidance, a financial institution's senior managers are responsible for understanding the risks associated with foreign-based outsourcing arrangements and for adopting effective risk management

² This FFIEC guidance is available at http://www.ffiec.gov/PDF/pr112800_guidance.pdf. See also, FFIEC Information Technology Examination Handbook's "Information Security Booklet" (Dec. 2002), "Supervision of Technology Service Providers Booklet" (March 2003), and "Business Continuity Planning Booklet" (March 2003) available at: <http://www.ffiec.gov/ffiecinfobase/index.html>.

³ Country risk is an exposure to economic, social, and political conditions in a foreign country that could adversely affect a vendor's ability to meet its service level requirements. In certain situations, country risks could result in the loss of an institution's data, research, or development efforts. Managing country risk requires institutions to gather and assess information regarding foreign political, social, and economic conditions and events, and to address the exposures introduced by the relationship with a foreign-based provider.

⁴ The Agencies, through the FFIEC, are developing uniform interagency guidance on use of foreign-based service providers and this response reflects that interagency effort. This guidance will appear in an appendix to the forthcoming "Outsourcing Booklet" for the FFIEC Information Technology Examination Handbook.

practices. These include appropriate due diligence, oversight and monitoring procedures. Management should determine if it can mitigate identified risks. Before contracting with a foreign-based entity, management should consider various issues, including choice-of-law, compliance, and jurisdictional considerations. The institution should consider both the usual risks associated with domestic service providers (which are present in foreign-based arrangements) and the unique risks arising from reliance on particular service providers that depend, for example, on the countries in which they are located.

With respect to privacy and security, the obligations of a U.S. financial institution to protect the privacy and security of information about its customers under applicable U.S. laws and regulations remain in full effect when the institution transfers or transmits the information to a foreign-based service provider. The transfer or transmission of that information to a service provider located in another country does not alter those obligations.

Risk Assessment. Preservation of the privacy and security of customer information is a compliance risk. An institution using a foreign-based service provider must still comply fully with requirements under applicable U.S. laws, including requirements relating to the protection of customers' nonpublic personal information under section 501(b) of the Gramm-Leach-Bliley Act (GLB Act).⁵ Institutions also should consider the impact and operational requirements of foreign data privacy laws or regulatory requirements.⁶

Due Diligence. The due diligence process should include an evaluation of a firm's financial stability and commitment to service, and the potential impact of the foreign jurisdiction's regulations, laws, accounting standards, and business practices on the privacy and security of customer data. Additionally, management should consider the degree to which geographic distance, language, or social, economic, or political circumstances may affect the foreign-based service provider's ability to meet the institution's servicing needs.

Contract Provisions. Contracts between a financial institution and its foreign-based service provider should address identified risks including those associated with the privacy and security of its customer information. Specifically, the institution should require contract provisions to protect its customers' information in conformance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (the "Guidelines") and other applicable requirements under federal law.⁷ For example, a contract with a service provider should include provisions requiring the provider to implement procedures and security measures that meet the specific objectives of the Guidelines, such as protecting against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer. Additionally, the forthcoming FFIEC Outsourcing Booklet provides that any agreement between a financial institution and a foreign-based service

⁵ 15 U.S.C. §§ 6801 and 6805(b).

⁶ Institutions should identify and understand the application of any laws within a foreign jurisdiction that apply to information transferred from the United States to that foreign jurisdiction or to information collected within the foreign jurisdiction using automated or other equipment in that jurisdiction.

⁷ 12 CFR 30, Appendix B, ¶ III.D.2; 12 CFR 208, Appendix D-2, ¶ III.D.2.; 12 CFR 225, Appendix F, ¶ III.D.2.; 12 CFR 364, Appendix B, ¶ III.D.2.; 12 CFR 570, Appendix B, ¶ III.D.2.; and 12 CFR Part 748, Appendix A ¶ III.

provider should provide that all information transferred to that provider remains the property of the institution. Contracts with a foreign-based service provider should contain a provision acknowledging the authority of the appropriate U.S. regulatory agency to examine the services performed by the provider.⁸

Monitoring and Oversight. Where indicated by its risk assessment, the financial institution must monitor its foreign-based service providers to ensure the continued privacy and security of customer information and to confirm that they have satisfied their contractual obligations to comply with the objectives of the Guidelines. This includes the ability to determine whether the provider maintains adequate physical and logical security controls⁹ to meet the objectives of the Guidelines, transaction procedures, business resumption and IT contingency arrangements, insurance coverage, and compliance with applicable laws and regulations.

Regulatory and Supervisory Oversight. The Agencies have also considered their ability to supervise foreign-based service provider relationships. U.S. financial institution regulatory agencies may review the services performed for an institution under an outsourcing arrangement with a foreign-based service provider. Likewise, in the case of a foreign-regulated entity, U.S. regulatory agencies may be able to obtain information through the appropriate supervisory agency in the service provider's home country. Generally, the Agencies' principal supervisory strategy in this area is to focus on the ability and obligation of the serviced financial institution to maintain adequate controls over those foreign-based service providers that handle its customer information. Accordingly, the Agencies will focus their respective reviews of an outsourcing relationship on the adequacy of the institution's due diligence efforts, its risk assessments, and the steps taken to manage those risks.

In light of this general discussion, we will now turn to your specific questions.

Information on use of foreign service providers by specific institutions. You have requested lists of U.S. banking institutions subject to the jurisdiction of the Agencies that transfer customers' nonpublic personal information to affiliated and non-affiliated foreign-based service providers. For each of the institutions on these lists, you request specific information on the information transferred, the purpose of the transfer, the nature of consumer disclosures provided by the entity with respect to the transfer, and whether the institution gives customers the ability to opt-in or opt-out.

None of the Agencies collects the information that you have requested and the Agencies do not anticipate collecting that information. Thus, we are unable to provide the institution-specific information you requested.

⁸ As noted in the October 2003 GAO Report on Credit Unions to the Ranking Minority Member, Committee on Banking, Housing, and Urban Affairs, U.S. Senate, NCUA does not have the authority to examine third-party vendors. Any reference to the Agencies' authority on this issue would not apply to NCUA.

⁹ Logical controls are controls incorporated in the hardware and software of an information technology ("IT") system that prevent, detect, and enable recovery from adverse actions that threaten the IT system's confidentiality, integrity, and availability. Logical controls include limited, controlled network access privileges and the monitoring/logging of network intrusion attempts.

Examinations focused on transfer of information to foreign service providers. You ask how many examinations have been conducted to determine whether outsourcing of nonpublic personal information to foreign-based service providers may have resulted in unauthorized disclosure, access or use of customer information. We are unable to give you the number of examinations that have been conducted because the Agencies do not conduct examinations specific to the purpose that you have outlined. However, as noted above, each of the Agencies conducts a review of information security practices and vendor management practices (for both domestic and foreign-based service providers) as part of the regular, ongoing supervisory activities.

Agency efforts to assure compliance with §501(b) of the GLB Act. We are providing an overview of the Agencies' process for supervising financial institutions' information security practices and vendor management to assist you in assessing the scope and effectiveness of supervision in this area. In promulgating regulations under section 501(b) of the GLB Act, the member agencies of the FFIEC established a process-based approach to regulating financial institutions' information security practices. The FFIEC Information Technology Examination Handbook, "Information Security Booklet," issued by the FFIEC in December 2002, adopts the same process-based approach to examination of financial institutions' information security systems and practices. Examiners may refer to the Information Security Booklet when evaluating the financial institution's risk management process for compliance with section 501(b) of the GLB Act. Depending on risk indicators, examiners evaluate, among other aspects of the financial institution's information security program, the adequacy of the institution's risk assessment of the service provider and its monitoring of the testing performed at the service provider such as whether management has reviewed timely audits regarding controls intended to protect customer information.

For a financial institution that places heavy reliance on third-party service providers, the supervisory strategy generally would include both an annual examination of, and ongoing supervision related to, the institution's vendor management processes. The use of foreign-based service providers would be one factor that influences the examiner's assessment of information security as well as transaction, strategic, reputation, compliance, and country risk for each institution.¹⁰

As discussed above, our supervisory approach to outsourcing emphasizes the responsibility of the serviced financial institution to conduct adequate due diligence, manage risks appropriately, comply with applicable laws and ensure access to critical information with respect to the services being provided, whether by a foreign-based or domestic entity. Therefore, our review of foreign-based service provider arrangements to date has been limited to interviewing institution staff and reviewing documentation (security policies, third-party security audits, financial statements, contracts, business resumption and disaster recovery

¹⁰ The Agencies' supervisory strategies consist of a combination of examinations and ongoing supervisory activities. Examination planning is based on the examiner's assessment of risk. An examination will target a specific control, line of business, or function within the financial institution and generally will include an evaluation of the level of risk in the targeted area, as well as the quality of controls in place to manage that risk. For example, an examination of a financial institution's vendor management processes would typically involve identifying mission critical service providers and evaluating the institution's vendor management practices.

plans, etc.), which must be maintained in English at a domestic office of the institution. To date, the Agencies have not identified any instances where the use of a foreign-based service provider has resulted in the unauthorized disclosure, access to, or use of customer information with respect to customers of insured depository institutions.

You also ask whether any enforcement actions have been undertaken to address violations of the privacy and security provisions of GLB Act or the Fair Credit Reporting Act (FCRA) with respect to U.S. financial institutions that provide customer information to foreign-based service providers. The Agencies have taken no such formal enforcement actions.

A description of the Agencies' process for taking enforcement actions may assist you in assessing the scope and effectiveness of the Agencies' supervisory activities in this area. When examiners identify weaknesses in a financial institution's vendor-management processes, a number of actions can be taken depending on the level of risk. Where the risk does not pose a threat to the safety and soundness of the institution and management is considered capable and willing to address the weaknesses in the normal course of business, the examiners will usually issue recommendations for management's attention and obtain a commitment to implement corrective action. Recommendations may also be included in the financial institution's Report of Examination. Subsequently, the examiners will monitor management's progress in implementing corrective action until the weakness has been resolved.

When key components of the vendor-management process are not in place, examiners may cite the financial institution for violating the Agencies' Guidelines. The violation would be noted in the Report of Examination as a Matter Requiring Attention or in other written correspondence to management.

If the vendor-management processes are severely deficient, the safety and soundness of the financial institution is at risk, or customers' nonpublic personal information is not adequately protected, the Agencies may take stronger supervisory action, such as requiring that the institution submit a written compliance plan, issuing a cease and desist order, and imposing civil money penalties.

Agency authority over foreign service providers and their employees. You have inquired whether the Agencies have the authority to bring a legal action against a foreign-based service provider in the event that the provider (affiliated or not affiliated with a U.S. financial institution) violates the privacy or security provisions of the GLB Act or the FCRA. You also ask what authority the Agencies would have to bring enforcement actions against a rogue employee of the provider company for violations that occurred in a foreign country.

The situation you describe would, in most cases, mean that the serviced institution has violated its obligations under U.S. laws or regulations to protect the privacy or security of its customers' information. Accordingly, the agency with primary supervisory responsibility for the serviced institution would have authority to take enforcement action against that institution for this violation. This action could result in an order that, among other remedies, directs the institution to exercise its contractual authority over the service provider to compel

action to correct the violation or to terminate the relationship. The Agencies presently have the ability to take public enforcement actions against institutions detailing deficient practices at a particular foreign-based service provider and, in appropriate cases, require alternative measures to protect information or termination of a servicing relationship with that provider. The ability to take these enforcement actions vests the Agencies with indirect influence over the conduct of the foreign-based service providers.

Depending on the circumstances, the primary agency may also have the authority to take a direct enforcement action against the foreign-based service provider. In most situations, the Agencies would not have authority to take direct enforcement action against the rogue employee of a foreign-based service provider. However, the ability to take effective action against the serviced institution should enable the Agencies to compel effective remedial action with respect to the rogue employee.

Customers' rights under the GLB Act or FCRA. You asked what legal rights and remedies an individual whose privacy had been violated or compromised by a foreign-based service provider would have under the GLB Act or the FCRA. The GLB Act does not provide for any private right of action against a financial institution, its service providers, or the employees of the institution or service provider for violations of the privacy provisions set forth in title V of the Act. Violations by a financial institution are subject only to enforcement action by the appropriate functional regulator or the Federal Trade Commission (FTC). Thus, an individual whose privacy rights may have been violated may direct a complaint against the financial institution to the appropriate regulator for investigation and action where warranted. Each of the Agencies has a mechanism for receiving and responding to complaints filed by consumers against the institutions supervised by the agency. Additionally, the Board, the FDIC, the OCC, and the OTS have authority under 12 U.S.C. § 1818 to order restitution to consumers. Similarly, the NCUA may take such action under 12 U.S.C. § 1786.

On the other hand, the FCRA provides a number of avenues for enforcing the various duties imposed under that statute. In addition to the authority of the federal banking agencies, the FTC, and certain other federal agencies to take administrative enforcement actions under 12 U.S.C. §§ 1786 and 1818, an individual may file an action. State officials may also bring actions on behalf of residents of their respective states. An individual also may pursue a cause of action against a financial institution for the actions of the institution's agent – in this case, the offshore company or the company's employee. The FCRA provides for recovery of actual damages, and in the case of willful noncompliance, for the imposition of statutory and punitive damages.